Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A system, comprising:

a control center ~~central controller system~~ to coordinate thwarting ~~denial of service~~ attacks on a victim data center that is coupled to a network ~~comprises:~~ the control center including:

a communication device to receive data from a plurality of monitors, dispersed through the network, with the monitors sending data collected from the network over a hardened, redundant network;

a computer system, the computer system comprising:

a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic.

2. (Currently Amended) The system of claim 1 wherein the control center ~~computer system~~ further comprises:

an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center.

3. (Original) The system of claim 1 wherein the data analyzed by the control center is sampled packet traffic and/or accumulated and collected statistical information about network flows.

4. (Original) The system of claim 1 wherein the control center aggregates traffic information and coordinates measures to locate and block the sources of an attack.

5. (Original) The system of claim 1 wherein the control center is a hardened site.

6. (Currently Amended) The system of claim 1 wherein monitors include gateways that are disposed at the victim data center and data collectors that are disposed in the network, and the analysis process executed on the control center analyzes data from gateways and data collectors dispersed throughout the network.

7. (Original) The system of claim 1 wherein the analysis process classifies attacks and determines a response based on the class of attack.

8. (Original) The system of claim 7 wherein the classes of attack are denoted as low-grade with spoofing, low-grade without spoofing and high-grade whether spoofing or non-spoofing.

9. (Currently Amended) A method comprises:

~~to coordinate~~ thwarting ~~denial of service~~ attacks on a victim data center that is coupled to a network; ~~comprises:~~

receiving data from a plurality of monitors, dispersed through the network, with the monitors sending data collected from the network over a hardened, redundant network; and

analyzing the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic.

10. (Original) The method of claim 9 further comprising:

determining a filtering process to eliminate the malicious traffic from entering the victim data center.

11. (Original) The method of claim 9 further comprising:

aggregating traffic information and coordinating measures to locate and block the sources of an attack.

12. (Currently Amended) The method of claim 9 wherein receiving and analyzing are performed by a control center coupled to the ~~data collectors~~ monitors via the hardened, redundant network.

13. (Original) The method of claim 9 wherein plurality of monitoring devices are data collectors dispersed throughout the network and at least one gateway device that is disposed adjacent the victim site to protect the victim and wherein analyzing comprises:

analyzing at a control center data from the at least one gateway and the data collectors dispersed throughout the network.

14. (Original) The method of claim 9 wherein analyzing comprises:

classifying attacks and determining a response based on the class of attack.

15. (Original) The method of claim 14 wherein the classes of attack are denoted as low-grade with spoofing, low-grade without spoofing and high-grade whether spoofing or non-spoofing.

16. (Currently Amended) The method of claim 14 further comprising:

sending requests to gateways and/or data collectors ~~for~~ to send data pertaining to an attack to the control center.

17. (Currently Amended) The method of claim 14 further comprising:

sending requests from the control center to gateways and/or data collectors for requests to install filters to filter out attacking traffic.

18. (Currently Amended) A computer program product to coordinate thwarting ~~denial of service~~ attacks on a victim data center that is coupled to a network comprises instructions to cause a computer to:

receive data from a plurality of monitors, dispersed through a first network that is coupled to the victim data center, with the monitors sending data collected by the monitors from the first network to a control center over a hardened, redundant, second different network; and

analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic.

19. (Original) The computer program product of claim 18 wherein instructions to receive and analyze are performed by a control center coupled to data collectors via a hardened, redundant network.

20. (New) The computer program product of claim 18 further comprising instructions to:

determine a filtering process to eliminate the malicious traffic from entering the victim data center; and

aggregate traffic information and coordinating measures to locate and block the sources of an attack.